Land Information Warfare Activity (LIWA)

1-1. RESPONSIBILITIES. The LIWA provides information operations (IO) support to Army active and reserve components (AC/RC), to facilitate planning and execution of military operations.

1-2. RELATIONSHIPS.

a. The LIWA is a major subordinate activity of the U. S. Army Intelligence and Security Command (INSCOM). The Commander of LIWA has a dual relationship with INSCOM and the Army Staff (ARSTAF). The LIWA is a subordinate command, and under administrative control, of HQ INSCOM. The Directorate of Operations, Readiness and Mobilization (DAMO-OD), ACofS, G3, Headquarters, Department of the Army (HQDA) exercises operational control of the LIWA, including operational support, policy and programming guidance.

b. The LIWA is authorized to have direct contact with the ARSTAF, the Army Secretariat, and the Defense Secretariat, field commands, the Joint Staff and other agencies on operational issues related to IO. LIWA communications with the Office of the Secretary of the Army and Office of the Secretary of Defense are sent through DAMO-OD for transmission through the DCSOPS, HQDA and the Director of the Army Staff.

1-3. MISSION AND FUNCTIONS.

a. Mission. Provide IO support to the Army; support the warfighter in planning, synchronizing and executing IO for the commander; enhance Army force protection through a proactive defense. As the operational focal point for IO in the Army, the LIWA plans, synchronizes, executes and assesses IO for worldwide Army warfighting and other commanders in garrison, on field training exercises and experiments, and in contingency operations. The LIWA provides and/or coordinates for the appropriate level of IO defense and IO attack, and IO-related support, to Army and other land component commanders (LCCs).

Figure 1-1 depicts the current LIWA organization.

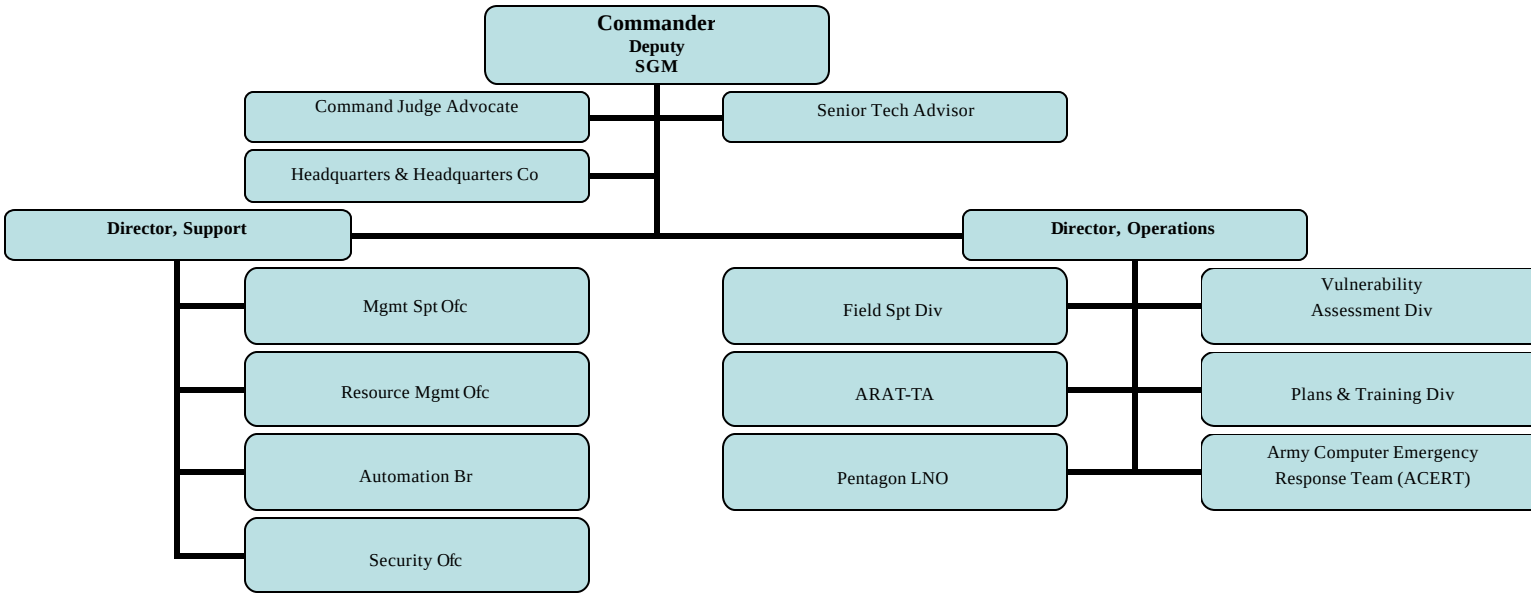

Figure 1-1. LIWA Organization

b. <u>Specified Functions</u> (with authority cited).

(1) Serve as operational focal point for land IO. (CSA MSG)

(2) Coordinate and deploy field support teams (FSTs) to assist LCCs in offensive and defensive IO. (CSA MSG)

(3) Act as the Army functional proponent for battlefield deception. (DCSOPS MSG).

(4) Coordinate and assist U.S. Army Training and Doctrine Command (TRADOC) in developing and integration of doctrine, training, leader development, organization, materiel and soldiers (DTLOMS) requirements for IO. (CSA MSG/MOU)

(5) Initiate and coordinate requirements for IO-related area studies (CSA MSG/MOU)

(6) Assist in the development and integration of IO requirements in Army Modeling strategy and policy scenarios and course of action analysis tools/modeling and simulation. (CSA MSG/MOU)

(7) Coordinate and synchronize IO intelligence and counterintelligence support. (CSA MSG/MOU)

(8) Assist in the development and evaluation of IO systems performance and operational employment tactics, techniques and procedures in battlefield operations, operational tests and training exercises. (CSA MSG)

(9) Establish, develop and promote IO interoperability with other Services and allies. (MOU)

(10) Assess IO force readiness and IO operational capabilities. (CSA MOU)

(11) Establish and operate the Army Computer Emergency Response Team (ACERT) and Regional CERTs. (HQDA IO Campaign Plan)

(12) Conduct tactical, operational and facility-level full-spectrum vulnerability assessments (VATs) of Army units, organizations and activities. (HQDA Cyber Intrusion Detection Action Plan)

(13) Conduct VA Penetration Testing and Red Teaming of Army units, organizations and activities. (HQDA Cyber Intrusion Detection Action Plan).

(14) Advise and assist combat and material developers in institutionalizing VAs during experiments, technology demonstrations and developmental tests and evaluations of all centrally procured, information technology-based systems. (HQDA Memo)

(15) Serve as the Army CND force component (ARFOR) of the US Space Command Joint Task Force for Computer Network ~~Defense~~ Operations (JTF-CN~~D~~O) for CND. (HQDA)

(16) Act as the Army's certification authority for Army information system (AIS) penetration testing IAW AR 380-53, Information System Security Monitoring (ISSM). (AR 380-53)

c. Mission-Essential Task List (METL).

(1) Establish, develop and promote IO interoperability by assisting CINCs, the Services, agencies and activities, Army and land component commanders to coordinate, plan, synchronize and execute full-spectrum IO.

(2) Conduct an active defense of Army Information and Information systems through relevant information correlation and vulnerability assessment, and manage the coordinate of the Army's computer network defense.

(3) Develop, war-game and recommend IO courses of action based on manipulation and synthesis of multiple data sources to support commanders to the field.

(4) Support efforts to define IO policy and procedure, and the development of IO doctrine, training, leader development, organization, materiel and soldier systems (DTLOMS) for HQDA and TRADOC.

(5) Support military operations by developing mission- and geographic-oriented electronic combat threat lists and parametric libraries for Army target sensing systems.

1-4. STAFF FUNCTIONS.

a. Office of the Commander. The Office of the Commander is charged with supervisory management of the LIWA's activities. The Commander sets policy, issues guidance and oversees the operations of the LIWA. The Commander is an integral player in Army IO with key personnel from HQDA DCSOPS; Deputy Chief of Staff for Intelligence (DCSINT), for intelligence and counterintelligence support to IO; and Director of Information Systems for Command, Control, Communications and Computers (DISC4), for information assurance/security. Other, assigned responsibilities include -

(1) Serving as the senior advisor to the Commanding General, INSCOM and the INSCOM Command Group, headquarters staff and major subordinate commands and activities for all matters concerning IO and its applicability throughout INSCOM.

(2) Maintaining operational IO coordination with the Joint IO Center (JIOC), Air Force IW Center (AFIWC), and Navy IW Activity/Fleet IW Center (NIWA/FIWC).

(3) Coordinating within the Army, and with other Services and national agencies for intelligence support to IO.

(4) Coordinating deployment of LIWA field support elements to assist Army and other LCCs to train, plan, coordinate and synchronize IO to support designated tests, experiments, exercises and operational contingencies.

(5) Coordinating, planning and executing operational IO requirements through the HQDA, ACofS, G3, for regional CINCs and LCCs.

(6) Serving as the Deputy Commander, ARFOR (DEPCOMARFOR) of the JTF-CND, using the assets of the LIWA ACERT Coordination Center (ACERT/CC) to conduct Army CND activities.

(7) Command Judge Advocate (CJA). The Command Judge Advocate for the LIWA provides legal advice to the Commander, LIWA and his staff. The CJA primarily advises the Command Staff on operational law matters. Operational law matters include intelligence law, information technology law and deployment authorities. The CJA also advises the Commander, LIWA on any other legal topics that arise including intellectual property law, military justice matters and labor law issues. The CJA serves as the LIWA Ethics Advisor and coordinates with the HQ INSCOM SJA and HQDA authorities on matter affecting LIWA. The LIWA CJA also serves as the IDC CJA.

(8) Headquarters & Headquarters Company (HHC). The HHC provides command and control, training management, administrative, logistical and UCMJ support to soldiers (officers and enlisted), government civilians, and contractors assigned or attached to the Land Information Warfare Activity, U. S. Army Intelligence and Security Command.

b. Deputy, LIWA (Deputy Director for Support)(DDS). The following offices and functions comprise the DDS, Management Support Office, Resource Management Office, Security Branch, and the Automation Branch..

(1) Management Support Office (MSO). The MSO is responsible for providing support to LIWA in all areas of force structure, manpower management, personnel and administration. The following functions are specified:

(a) Manage the force structure and integration process

(b) Plan, coordinate and conduct manpower surveys for the LIWA

(c) Coordinate and develop the LIWA authorization documents

(d) Produce and update the LIWA organizational, mission and functions documentation

(e) Manage the military and civilian personnel management systems for the LIWA

(f) Manage the military personnel requisitions and civilian hiring for the LIWA

(g) Represent LIWA at INSCOM and other higher-level manpower and force structure meetings

(h) Develop LIWA policy letters and administrative procedures

(k) Manage the LIWA Sponsor Program

(l) Maintain the LIWA Publications Library

(m) Administer the LIWA personnel rating schemes

(n) Manage the LIWA military and civilian awards programs

(o) Manage and coordinate the LIWA Reenlistment Program

(p) Manage incoming and outgoing mail and distribution

(q) Manage and coordinate the LIWA Soldier Readiness Processing (SRP)

(r) Coordinate SIDPERS interface with the G1/HQ Commandant, HQ, INSCOM

(2) Resource Management Office (RMO). The Resource Management Office provides financial, contracting and logistic support to the Commander, Deputy, its Support Staff and four Operations Divisions. The RMO is currently authorized one Military, five Civilians and four Contractors to support LIWA's requirements.

(a) Financial Management. The RMO is responsible for the development, coordination and submission of LIWA's program documents; and the coordination, formulation and execution of the LIWA's operating budget. Other financial functions:

- Conducts liaison with INSCOM - ACofS, Resource Management (RM); HQDA - DCSOPS, DCSINT, DISC4; and other agencies, as appropriate, concerning resource management issues
- Serves as centralized program coordinator for all LIWA financial programs
- Advises on resource management matters
- Prepares and defends the LIWA resources requirements
- Manages and analyzes the execution of OMA and RDTE funds for which LIWA has execution authority
- Analyzes LIWA programs and budget guidance and provides guidance to Commander, Deputy Directors and division chiefs
- Performs program and baseline resource evaluations to identify resource trade-off and low-benefit activities
- Develops LIWA policy and administers INSCOM's RM program IAW pertinent Army regulations

(b) Contracting Support. The RMO is the principal advisor to the Commander and Deputy on acquisition matters. Responsible for the LIWA Acquisition Plan, development of procurement packages, monitoring contracts/contractors performance, including expenditure rates, and preparing contract modifications. Other contracting functions:

- Develop, coordinate and monitor LIWA contracts IAW Federal, DOD and Army procurement policies, directives and procedures
- Prepare and coordinate all contract modifications
- Perform Contracting Officer's Representative responsibilities for all LIWA contract actions
- Serve as contract security monitor for all LIWA contracts
- Establish and implement comprehensive acquisition planning procedures for the LIWA

(c) Logistics Support. The RMO is the principal advisor to the Commander and Deputy Director on all logistics matters. Responsibilities include property accountability, maintenance, transportation and disposal. Other logistic duties:

- Coordinate the procurement, identification, control and accountability of all LIWA equipment
- Maintain the LIWA's hand-receipts and issue sub-hand-receipts
- Coordinate for the maintenance of LIWA equipment and facilities
- Coordinate packing, crating and transportation of LIWA deployable equipment
- Identify property for disposal
- Operate and maintain the LIWA Arms room
- Coordinate all LIWA Intra-service Support Agreements
- Monitor Command Supply Discipline Program (CSDP)

(3) Security Branch. The Security Branch is responsible for developing and implementing information, personnel, computer, operations and physical security

programs required to support LIWA administrative and operational activities. Duties include:

(a) Serving as the Activity Security Manager with organizational responsibility for security matters related to the LIWA

(b) Monitor the activity OPSEC program; implement OPSEC guidance from higher headquarters

- Implementing and managing the LIWA information security program to include: Providing classification and declassification guidance and oversight
- Developing and implementing the L IWA security education and awareness program
- Developing policies, procedures and guidance for the storage, control, and disposition of classified materials within the LIWA
- Conducting preliminary inquiries into collateral and special compartmented information (SCI) security violations/incidents
- Establishing and maintaining document control procedures and accountability systems for the LIWA

(c) Implement and manage the industrial security program for contracts administered by the LIWA to include administration of contractor SCI billets, review of contract security specifications and determination of classification requirements.

(d) Develop, implement and manage the LIWA personnel security program to include:

- Managing the LIWA SCI billet structure: assignment of billet numbers, monitoring the status of periodic reinvestigations (PRs) required, submitting SCI nominations, submitting "compelling need" requests, requesting transfers-in-status and maintaining SCI access rosters
- Submitting annual and “as required” permanent and/or visit clearance certification messages for access to SCI and collateral information
- Maintaining liaison with the INSCOM Special Security Officer (SSO) for the purpose of coordinating SCI indoctrinations,

clearance certifications, SCI courier orders, in-out processing and other functions charged to the SSO

- Monitoring projected gains and notifying SSO INSCOM of clearance status

- Approving collateral courier orders for CONUS travel of LIWA personnel

(e) Serve as the LIWA NATO material custodian.

(f) Serve as Special Access Program (SAP) Security Manager for those SAPs for which the LIWA is the designated proponent, performing those duties specified in AR 380-381. Serve as an Access Approval Authority for those SAPs for which the LIWA is a participant but not the designated proponent. Responsibilities include:

- Maintaining access rosters for LIWA personnel indoctrinated for SAPs

- Monitoring status of special background investigations/PRs for LIWA personnel accessed to SAPs

- Maintaining document control/accountability systems for SAP information

- Conducting SAP indoctrinations/debriefings as required

(g) Coordinate and conduct physical security responsibilities as required or directed in support of the LIWA mission; maintain liaison and coordination with supported MACOMs on behalf of LIWA elements operating under the security cognizance of such MACOMs.

(h) Develop, coordinate, review and implement IO security policy directives, regulations and guidance as directed by the Commander and/or Deputy Director, LIWA.

(4) Automation Branch. This element manages the LIWA's extensive automated information and communications systems in support of LIWA operations. In addition to operating and maintaining the INSCOM IDC, this branch of the Information Division is responsible for:

(a) Planning, formulating and validating information and communications systems requirements in support of the LIWA

(b) Planning, coordinating, installing and maintaining the communications and automated information infrastructure in support of LIWA liaison, deployed and other non-resident and elements of the LIWA

(c) Planning, coordinating and operating special IO systems in support of land and Army component commanders in exercise and contingency operations

The branch is responsible for the operation and maintenance of the following connectivities in support of the Commander, LIWA role as COMARFOR in the US Space Command's JTF-CND.

- Non-secure internet protocol (IP) router network (NIPRNET)
- Secret IP router network (SIPRNET)
- Global Command and Control System (GCCS)
- Joint Worldwide Intelligence Communications System (JWICS)
- Automatic Digital Network/Defense Message System (AUTODIN/DMS)
- NSA secure phones
- DoD RED switch phones
- Secure Telephone Unit III/Defense Systems Network (STUIII/DSN) Phones
- JWICS video teleconferencing (VTC) (access)
- FAX (CLASS/UNCLAS)

c. Deputy Director for Operations. The Deputy Director for Operations (DDO) directs, schedules, coordinates and synchronizes operational planning, training and execution to meet the full spectrum of Army, other LCCs' and specified joint IO requirements. Directly responsible to the DDO for functional staff support are the Situation Awareness Cell, Reserve Affairs Office, Activity Integration Office and ARAT-TA. The Plans and Training Division, as well, is subordinate to the DDO.

Under the DDO, the functional, operational divisions - the ACERT, Field Support (FS), IO Vulnerability Assessment (IOVA), and Plans and Training Divisions, and the Army Reprogramming Analysis Team - Threat Analysis (ARAT-TA) - provide operational planning, synchronizing and executing IO support to the Army, other LCCs and joint commands.

(1) Situational Awareness Cell. This DDO branch is responsible for coordinating and maintaining master scheduling for all LIWA operational activities. The branch tracks Army and joint worldwide activities (exercises, experiments, contingency operations, etc.) in which LIWA participation is requested, proposed, anticipated or implemented. Recommendations for accommodating LIWA operational commitments are synchronized with LIWA resource managers and supported commands. Current operations personnel operate from the INSCOM Information Dominance Center (IDC).

(2) Reserve Affairs Office. The Reserve Affairs Office serves as the single source for information regarding the integration of reserve component (RC) soldiers, both Army National Guard and Army Reserve, into LIWA operations. The reserve affairs office performs a variety of tasks in support of this overreaching mission.

(a) During non-mobilization periods, the reserve affairs office:

- Performs liaison functions with LIWA divisions, identifying missions suited to unique RC capabilities and provides RC soldier augmentation to accomplish these missions.
- Develops, implements, and monitors AC/RC integration initiatives for the unit
- Serves as the unit's subject matter expert for reserve specific issues (force structure, missions and capabilities, personnel and duty policies, training, etc.)
- Serves as the unit's RC liaison t outside agencies (INSCOM, FORSCOM, USARC, OCAR, NGB, etc.

(b) During periods of mobilization, the reserve affairs office:

- Coordinates the identification and resourcing of available RC assets to fulfill critical shortfalls in the LIWA's operational capabilities.
- Monitor, interprets and disseminates mobilization related policies and procedures to mobilized RC soldiers/units and the LIWA staff as appropriate.
- Provides coordinated staff recommendations to the LIWA command group relating to mobilization matters and the employment of mobilized RC elements.

- Serves as LIWA liaison to outside mobilization agencies including but not limited to Army G3, FORSCOM, INSCOM, USARC, NGB and selected mobilization installations.)

(3) Liaison. Under the DDO, LIWA liaison activities on IO matters consists of representation to, and/or interface and coordination with, the ARSTAFF and Joint Staff in the Pentagon, Joint Warfare Analysis Center at the Naval Surface Warfare Center, Dahlgren, VA; Joint Information Operations Center at the AFIWC; and Central Intelligence Agency. These liaisons allow the LIWA to leverage the capabilities of other organizations in support of the execution of LIWA missions and help reduce the potential for duplication among IO players.

d. ACERT Division. This element of the LIWA is charged with coordinating the conduct of CND and IA for Army active and reserve components across the full spectrum of military operations. The ACERT Coordination Center (CC) is designated as the ARFOR operational element in the US Space Command JTF-CNO. The division is organized with three branches: the Coordination Center (CC), Computer Defense Assistance (CDA), and the RCERT branches and five regional teams (RCERTs – CONUS, Europe, Pacific, Korea, Southcom and Southwest Asia (SWA). The RCERTs provide forward and installation commanders a quick-reaction, computer security incident-handling capability, Computer and Network Vulnerability Assessment, analysis, training and penetration testing and provide regional expertise to system administrators in proper system configuration, countering computer attacks and conducting post-attack assessments. ACERT functions are as follows:

(1) Report status of intrusions into Army AIS, vulnerability posture and trends to the Army leadership (HQDA).

(2) Provide assistance to system administrators concerning the protection of information resources through incident handlers at the ACERT/CC and information security specialists at the ACERT-CDA and the RCERT locations

(3) Respond to all Army computer security incidents, unexplained outages, denial of service, loss of accountability or presence of computer viruses

(4) Maintain a central incident reporting, vulnerability assessment and assessment mission management databases, software tools for assessing system vulnerabilities and guidelines for maintaining and operating AIS security

(5) Provide proactive support in assessing and enhancing system security capabilities through the use of network intrusion tools, and the vulnerability assessment tools incorporated into the Computer Defense Assistance Program (CDAP), while analyzing data from incidents, surveys, assessment data, and network intrusions.

(6) Manage the computer-centric CDAP IAW AR 380-19 and 380-53 to ensure compliance with information assurance ,vulnerability assessment , and penetration testing.

(7) Manage the Army-wide Vulnerability Assessment Certification training program to include certification authority for Army Information system (AIS) penetration testing.

(8) Provide technical support to joint, DoD and National CERT/CDAP missions

e. FS Division. The FS Division coordinates and deploys LIWA Field Support Teams (FSTs) to assist and support the land component commands in offensive and defensive IO. The FSTs provide responsive IO analysis, planning and targeting support to augment designated LCCs. When deployed, the FST becomes an integral part of the supported command's IO staff, filling gaps and coordinating with IO cells/staffs at the JTF or theater levels and other component commands in the operational area. FSTs also assist the supported command in employing LIWA VA Red Team, ACERT and ARAT-TA support, and help to develop a comprehensive picture of the command's IO strengths and vulnerabilities. FSTs deploy to support operations ranging from peacekeeping to major regional conflicts, and work closely with supported commands from the early planning stages to the completion of a military operation. Operational planning, wargaming, exercises and training programs are also supported. Functions include:

(1) Assisting in preparation of war plans, contingency plans and orders

(2) Assisting in the synchronization of the IO elements to accomplish specific IO warfighting objectives

(3) Assisting in the development of IO target lists, estimates and assessments

(4) Supporting analysis of the adversary's information infrastructure to include vulnerabilities and capabilities

(5) Assisting in the analysis and preparation of combat assessment and measures of effectiveness reporting pertaining to IO

(6) Providing defensive IO technical support.

(7) Assessing computer and communications disruptions with respect to adversary offensive IO capabilities

(8) Providing recommendations on how and when to employ assets in support of IO, to include those of other Services and agencies

(9) Coordinating with LIWA Information Division for intelligence support to field IO activities

(10) Supporting vulnerability assessments of friendly operations by identifying how an adversary may attack friendly information or information systems

(12) Supporting IO by revealing adversary deception operations

(13) Assisting in evaluation of IO effectiveness during execution

f. VA Division. The VA Division provides full-spectrum, multi-disciplined IO vulnerability assessments using Vulnerability Assessment Teams (VAT). These assessments are not inspections, but provide direct support to requesting commands, units and activities with a report going to the customer only, normally within 30 days of the on-site visit. The VAD has two Blue VA teams and one Red Team (Opposing Force (OPFOR)). The Blue Teams use interview processes, document reviews, direct observation and information system scanning tools, to assist Land Component Commanders identify and mitigate IO vulnerabilities to improve unit IO posture and force protection. The teams are tailored and usually consist of 8-10 personnel with 10-14 days on the ground assessment time. The teams attempt to locate the following:

(1) Vulnerabilities in the overall IO process including desynchronization of the pillars of IO within the unit. Pillars include Computer Network Defense, Computer Network Attack, Operations Security, Psychological Operations, Civil Affairs, Public Affairs, Deception, Electronic Warfare and Physical Strikes.

(2) Vulnerabilities in organizational and security structure, policy, programs and information flow.

(3) Weaknesses in the information infrastructure, to include the unit's ability to accomplish critical mission functions

(4) Vulnerabilities to enemy intelligence, deception, signals intelligence and psychological operations activities

(5) Vulnerabilities identified in the unit's Operations Security process including the capability of conducting Information Systems Security Monitoring of unit information systems (computers, phones and unsecure radios) to identify potential loss of Essential Elements of Friendly Information (EEFI).

The VATs (Blue Teams) also provide limited, on-site, hands-on assistance and training to minimize or eliminate vulnerabilities encountered during assessments. The VA Red Team simulates OPFOR capabilities targeted against a unit's information, information systems and decision cycle. Red Team operations provide training to the unit in Defensive IO including Computer Network Defense or operate in direct coordination with OPFOR for exercises. Red Team operations are recommended

following a Blue Team assessment in 3 to 6 months. This allows the unit to address vulnerabilities discovered by the Blue Team and the Red Team to verify the mitigating measures taken by the unit.

g. ARAT-TA. The Army Reprogramming Analysis Team – Threat Analysis (ARAT-TA) Activity is the element of the LIWA responsible for providing Electronic Warfare (EW) reprogramming support to operating forces and materiel developers. ARAT-TA identifies and reports changes in worldwide threat signature information that may affect the operation of EW and other Army target sensing systems (ATSSs). The LIWA ARAT-TA main element is collocated with the USAF 68th Electronic Warfare Squadron, 53rd Electronic Combat Wing, Eglin AFB, FL with a detachment at the AFIWC, Lackland AFB TX. The ARAT-TA:

(1) Monitors worldwide threat signatures to detect threat changes that affect ATSSs.

(2) Conducts impact assessments of signature changes.

(3) Maintains direct communications with national level intelligence agencies, the scientific and technical intelligence centers, and joint and service reprogramming centers in support of the rapid reprogramming effort

(4) Works with the Army's TRADOC centers and schools responsible for ATSSs to develop tactics, techniques and procedures to counter threat systems

(5) Participates in various RDT&E efforts to ensure a threat analysis capability is available to support advanced ATSS when the system is fielded.

h. Plans and Training Division.

(a) Plans Branch. The Plans Branch provides short, mid and long-range planning for all LIWA operational requirements and commitments.

The branch acts as a clearinghouse for requests for support from Army commands and participates in planning conferences to plan the scope of deployment and redeployment of active and reserve components' Field Support Teams (FSTs), Vulnerability Assessment Teams (VATs) and other support personnel - to include personnel from other commands/agencies. Other functional responsibilities are listed below.

- Monitor the status of deployed teams;
- Employ personnel with the appropriate skills to provide reach-back planning and targeting support for FSTs, VATs and supported units;

- Coordinate support from other LIWA elements;
- Recommend the selection and assignment of LIWA resources to fit requests for support from outside organizations; and
- Orchestrate assistance to supported commands for the development of the IO inputs to plans and orders.
- Special Technical Operations (STO)

The branch's Regional Section provides the LIWA interface for full-spectrum IO planning in support of the Land Component Commander (LCC). LIWA's planning support encompasses Regional and STO subject matter experts (SMEs) focused on support to the LCC war fighters in each combatant command. Planners in LIWA are both regional and technology focused SMEs who provide planning/special planning perspectives to LIWA's full-spectrum information operations (IO) missions. STO Planners coordinate with and support LIWA regional planners, their supported commands as required and other Army elements including INSCOM, Army STO office, Army Space Command/Space and Missile Defense Command staff, and Army DCS G3 staff, to achieve optimum visibility, inclusion, and integration of all IO capabilities into supported commands' IO campaign plans.

The Army Transformation Section of the branch is staffed to support the development of IO requirements in the tests, experiments and evaluations under the scope of the Army Transformation Experimentation Campaign Plan and transition to the Army Objective Force.

The Strategic Plans Section of the branch includes strategic IO planners and the LIWA Liaison Officer at HQDA who are responsible for LIWA strategic IO integration and coordination at the Joint Staff, Service departmental, DoD inter-departmental, inter-agency and multi-national levels. This cell is the planning focal point for IO and IO-related activities involving multiple combatant commands, and includes senior strategic planners with the knowledge, experience and stature to provide advice and mentorship for the strategic and unified combatant command planners.

The Operational Plans Section of the branch is responsible for integration and coordination of operational LIWA IO support to UCP-designated commands and their respective LCCs. This cell also includes senior operational-level planners with the knowledge, experience and stature to provide advice and mentorship with the emphasis on operational and Service-oriented planning.

The LIWA Detachment - Fort Meade (LIWA – Meade Section*)* represents the branch and is responsible for coordination and execution of planning and operations with the joint Services' IO Technology Center (IOTC), National Security Agency and other elements located at Ft Meade, MD. The IOTC focuses on US efforts

to develop and apply telecommunications and computer technologies to national security problems in the IO arena. The LIWA element is engaged in assessment and analysis of IOTC programs, activities and studies for possible impact on Army IO development and operational activities.

(b) Intelligence Branch. The branch is responsible for tracking and interpreting worldwide geopolitical developments and military movements for situational awareness of events/activities that might affect IO or IO-related indications and warning for friendly warfighting/peacekeeping forces. The focus of this branch's activity is IO and IO-related support to the regional planners residing in the Regional Section of the branch.

The primary effort of the Intelligence Branch is assigned to its Regional Intelligence Section, staffed with regional and transnational intelligence counterparts who support the regional IO planners associated with the unified combatant commands. The section is responsible for coordinating intelligence requirements, prioritization, planning, analysis and integration to meet the full spectrum of IO requirements for the combatant force commanders.

The other functional element of the Intelligence Branch is the General Support (GS) Intelligence Section, with its assigned complement of multi-disciplined, all-source intelligence specialists, who provide GS-level intelligence support to the regional intelligence specialists in the Regional Intelligence Section.

Specific, related functional activities for which the Intelligence Branch is responsible are as follows.

- Maintain close coordination with intelligence elements in the Intelligence Operations Center of the INSCOM IDC;
- Coordinate regional IO target data, targeting activity and determinations of intelligence gained/lost in the process of regional IO planning and execution;
- Initiate, coordinate and facilitate regional threat analyses and interpretations of enemy and potential enemy centers of gravity, critical decision nodes, vulnerabilities, defeat criteria and combat assessment and related reports;
- Provide point of access and dissemination for regional planners to selected IO and IO-related intelligence databases;

- Process and distribute regional commands' statements of IO-related intelligence interest and Intelligence Community responses;

- Support the preparation of priority IO and non-traditional target lists and estimates for regional combatants;

- Maintain regional libraries of area studies, incorporating military, economic, political, cultural, social and historical databases, for exploitation in support of theater and ASCC IO activities; initiate data mining, as required, using regional-based and other sources; and

- Provide, as required, reach-back, split-based IO-focused intelligence support to deployed LIWA elements.

(c) Requirements and Doctrine Branch. This branch is responsible for assisting HQDA and TRADOC in the development of Army IO doctrine; insuring that IO subject matter expertise resident in the LIWA assesses the evolution of Army doctrine and TTP; and reviewing DoD, joint and other Service doctrinal, material and combat development efforts that impact on Army practices. Another branch responsibility is contributing to the development and integration of full-spectrum IO requirements in Army TTP and scenarios. The branch identifies and documents IO weaknesses and solutions to TRADOC for the development of IO and IO-related DTLOMS.

The LIWA Exercise and Training Integration Center (ETIC), located at CAC, Ft Leavenworth KS, is a functional element of the Requirements and Doctrine Branch. The ETIC provides on-site subject matter expertise at CAC for IO doctrine development, exercise evaluations and IO professional development at the CAC institutions of higher military learning. The ETIC advocates and promotes TRADOC acceptance of and support to LIWA initiatives and products, and full-spectrum IO integration into the institutional Army. Specific functions of the ETIC include the following activities.

- Interface with CAC to identify and assess the impact of DTLOMS shortfalls, and the development of corrective strategies and programs;

- Support the Command and General Staff College (CGSC) by providing IO expertise and input to education and instruction programs: School of Advanced Military Studies program and the annual "Prairie Warrior" command post exercise for CGSC students;

- Work with the Center for Army Lessons Learned (CALL) to develop and maintain an IO folder in the CALL database;

- Maintain close coordination with the National Simulation Center to integrate IO into current and emerging models and simulations; and

- Interface with the Battle Command Training Program organization to integrate IO into the Army's premier force-on-force training program;

(d) Training, Education and Readiness (TE&R) Branch. The TE&R Branch is responsible for all facets of training (i.e. researching, managing, developing, presenting, scheduling) for the LIWA and IWEC. The Branch serves as the POC for input in developing IO-related doctrine. The Branch maintains close contact with the US Army's TRADOC, service schools, supported commands, and other services / agencies involved with IO/IW-related training, and doctrine development. To meet these responsibilities The Branch administers a comprehensive IO training, training / curriculum development, and training management program for the LIWA.

Training includes orienting/integrating newly assigned personnel, sustainment training for the various skills across the LIWA, specialized training for technical personnel, and LIWA-sponsored training available to the Army at large. Specific functions in the Training area include the following activities.

- Conduct semi-annual Army Battlefield Deception Planners Seminar (ADPS). This course is made available to the Army at large.

- Conduct quarterly Information Operations Capabilities and Planning (IOCAP) course. This course is made available to the Army at large.

- Conduct mission specific (e.g. Kosovo, Bosnia) Practical Exercises (PE) supporting readiness of deploying teams

- Conduct MTTs for IO-related training (e.g. ADPS, IOCAP, Centers of Gravity (COG) Seminar) upon request from the Army at large

- Conduct tailored, specialized training in support of LIWA divisional requirements

- Provide an IO Computer Based Training (CBT) CD for the LIWA, the Army-at-large and other Government agencies/activities.

Training/curriculum development involves the analysis, design, development, documentation, maintenance and updating of IO-related curriculum, courses, course materials, and practical exercises using various media. Training/curriculum development is constantly evolving to meet the latest doctrine and tactics, techniques and procedures (TTP) for IO in the Army. Specific functions in the Training/curriculum Development area include the following activities:

- Maintain/update the course content and materials for LIWA-sponsored training (e.g. ADPS, IOCAP, Centers of Gravity (COG), IO CBT CD, Regional PE)

- Develop the LIWA FA30 Enrichment Program

- Coordinate with TRADOC on course development, validation and standardization requirements

- Integrate web-based/computer-based formats into the training program

- Develop new courses and seminars to meet the needs of LIWA in maintaining subject matter expertise in IO.

Training Management focuses on monitoring and coordinating all of LIWA's training requirements as well as implementing and standardizing training-related policies and procedures. Specific functions in the Training Management area include the following activities: act as the Army's proponent for Battlefield Deception; act as the Army's training proponent for OPSEC; integrate/manage commercial- and government-sponsored Distance Learning training opportunities; maintain the Civilian Training Program; and, implement the Quality Assurance and Evaluation Program.